POSITION CLARITY · PLAIN-ENGLISH CRYPTO EDUCATION

How Networks *Agree*

A field guide to blockchain consensus for people who own crypto but were never told how these networks actually decide what is true. Five networks, five very different answers, and what each one is really good for.

Bitcoin Ethereum XRP Solana Hedera

Position Clarity

An educational reference.

POSITION CLARITY

Contents

SECTION 01

The problem blockchain is actually solving

Before we can talk about how five networks reach agreement, we need to be honest about the question they are all answering. It is a surprisingly old one: how do you move value, or agree on a record, when nobody at the table fully trusts anybody else?

Think about what happens when you send someone money today. You tap a button, and somewhere in the background a bank, a card network, or a payment app such as PayPal updates a list. That list says you have a little less and they have a little more. The whole system works because everyone agrees to treat that institution's list as the official one. The bank is the **middleman**, the trusted party in the middle that keeps the master record and settles disputes.

That arrangement is convenient, and most of the time it is fine. But it comes with quiet costs. The middleman can freeze your account, reverse a payment, make an error, charge a fee, close on a holiday, or simply tell you no. You are trusting one organization to be honest, accurate, and available. For a lot of the world, and a lot of situations, that trust is not a safe assumption.

The double-spend problem

So why not skip the bank and just send digital money directly, the way you send a photo? Here is the catch, and it is the heart of the whole field. A photo is just data, and data copies perfectly. If money were just a file, you could send the same file to ten people at once, or send it to a friend and still keep a copy for yourself. Spending the same unit of money twice is called the **double-spend problem**, and it is the reason digital cash did not work for decades.

In the bank world, double spending is impossible for a boring reason: there is one master ledger, and the bank checks it before every payment. A **ledger** is simply the running list of who owns what. One authoritative list, one source of truth, problem solved. The cost, again, is that you have to trust whoever holds the list.

> **THE CORE QUESTION**
>
> If you remove the trusted middleman, who keeps the ledger? If everyone keeps their own copy, whose copy is correct when two copies disagree? Answer that, and you have invented a blockchain.

A **blockchain** is one shared ledger that thousands of strangers maintain together, with a strict set of rules that makes them converge on a single agreed version, batch by batch. Each batch of transactions is a **block**, and each block is mathematically chained to the one before it, which is where the name comes from. Tampering with an old block would break every block after it, in plain view of everyone. There is no master copy to attack, because everyone has the same copy.

The nuance most explanations skip

It is tempting to say blockchains are "trustless." That is not quite right, and the real story is more interesting.

> *Blockchain does not eliminate trust. It redistributes it.*

Instead of trusting one bank not to make a mistake, freeze your funds, or quietly change the record, you are now trusting something different: that a majority of the network's **validators** will not coordinate to cheat at the same time. A validator is just a participant that helps check transactions and agree on the official record. Trust did not disappear. It moved, from a single named institution you can sue, to a large crowd of independent participants who would all have to collude to break the rules.

That shift is the entire point, and it is also the entire debate. How many validators do you need? How do you stop them colluding? How do you make cheating expensive and honesty profitable? How fast can a crowd of strangers agree without a boss? Every network in this guide is a different answer to those questions. The procedure each one uses to get that crowd to agree has a name: consensus.

SECTION 02

What "consensus" actually means

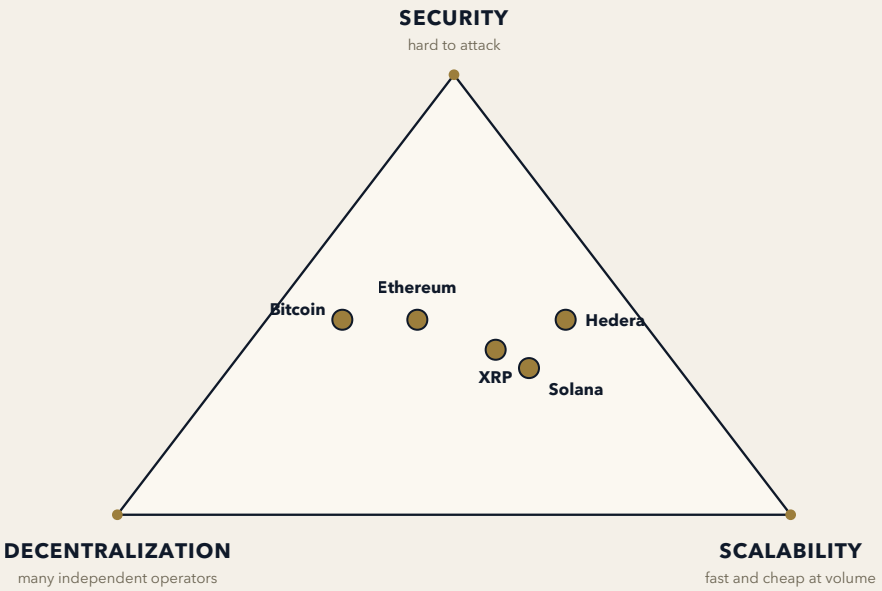
Consensus is the mechanism that solves the problem from Section 01. It is the agreed procedure a leaderless network uses to settle, over and over, on one official version of the ledger that everyone accepts.

Picture a few thousand strangers around the world, each holding a copy of the same notebook, with no manager and no head office. Every few seconds a fresh batch of transactions needs to be written into every copy, in the same order, with no disagreement. There is no one to break a tie. The rules themselves have to produce the tie-break. That set of rules is the **consensus mechanism**.

A good consensus mechanism has to do two hard things at once. It has to let honest participants agree quickly even though messages arrive out of order and some participants are offline. And it has to make sure a dishonest minority, or even a fairly large dishonest group, cannot force a false version of the record onto everyone else. Doing both, among strangers, with real money on the line, is genuinely difficult. That difficulty is why so many different designs exist.

> **THE FOUR LEVERS**
>
> Every consensus design is balancing four things that pull against each other: **security** (how hard it is to attack), **speed** (how fast payments settle), **decentralization** (how many independent participants, and how easy it is to join), and **programmability** (whether the network can run apps, not just move a coin). You cannot turn all four to maximum at once. Push one up and you usually give a little back somewhere else.

Three of those four levers pull against each other so reliably that the tension has a nickname: the **blockchain trilemma**. Those three are security, decentralization, and scalability (the speed-and-volume one). The rough rule is that you can have any two in full, but maxing all three at the same time is the hard, still-unsolved part. Programmability sits apart, a separate design choice rather than a third corner of the triangle.



Reading the triangle. Each corner is one thing a network can be best at. Because no network can sit in all three corners at once, each one lands somewhere inside, leaning toward the corners it chose. Bitcoin hugs the security and decentralization edge; Solana and Hedera lean hard toward scalability; XRP sits between, fast but more curated. These are directional placements to show the trade-off, not precise scores, and newer designs keep trying to push the whole triangle outward.

This is why there is no single "best" network, only different bets. The five networks ahead were chosen precisely because they make those bets differently, not because of how large they happen to be at any moment. Read them as five honest attempts at the same impossible-to-perfect problem.

- **Bitcoin** spends real electricity to make cheating expensive, and prizes security and openness above all.
- **Ethereum** makes validators post a cash bond instead, and trades some speed for the ability to run programs.
- **XRP** uses a circle of known, trusted validators to settle value in seconds.
- **Solana** timestamps everything up front so it can go very fast.
- **Hedera** throws out the single line of blocks entirely and uses a gossiping web.

READING FINALITY

"Final" does not mean the same thing on every network. Four flavors turn up in the pages ahead, and it is worth keeping them straight.

- **Probabilistic** (Bitcoin): a payment is never stamped final, it just gets harder to reverse as more blocks pile on top. You wait for it to be buried deeply enough.
- **Economic** (Ethereum): a block becomes final once reversing it would mean destroying an enormous amount of staked value. Final because the attack is ruinously expensive, not because it is impossible.
- **Confirmed is not final** (Solana): a transaction is confirmed in a flash once a supermajority votes, then finalized a little later once it is buried deeply. The fast number is confirmation, not finality.
- **Deterministic** (XRP, Hedera): once the trusted validators agree on the order, the result is final in one step, with no waiting for it to settle. This holds under the network's trust assumptions.

NETWORK 01 / 05

Bitcoin

PROOF OF WORK

Spend real electricity to make cheating expensive. Security and openness come first, and speed comes last.

WHERE IT LEANS · DIRECTIONAL, NOT A SCORE

* Decentralization is a theoretical ceiling. In practice a few mining pools command most of the hashrate, which concentrates who actually builds blocks.

Bitcoin

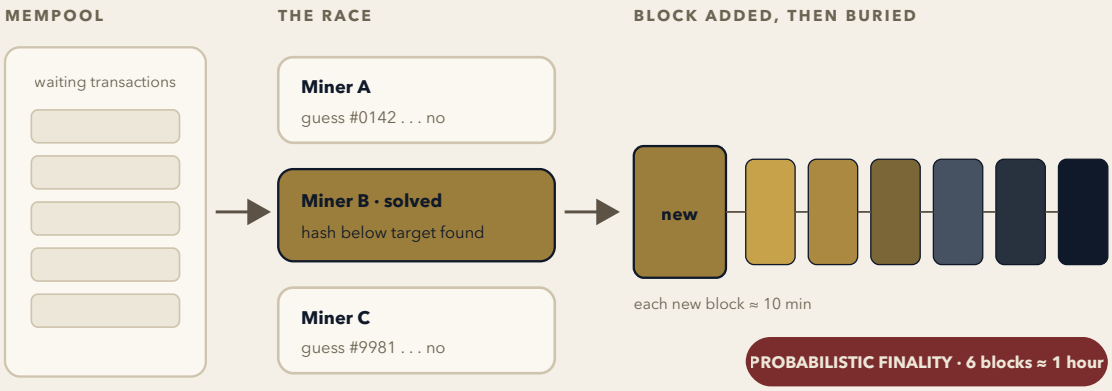
PROOF OF WORK · BTC

The original design. Security and openness first, speed last, paid for with electricity.

The mechanism, by analogy

Imagine a worldwide lottery that runs every ten minutes, except you cannot just buy a ticket with money. The only way to enter is to spend electricity. The players are called **miners**, computers competing for the right to add the next block. They all race to solve the same puzzle, and the puzzle has no clever shortcut. You simply guess, trillions of times per second, until someone stumbles onto a winning answer.

The puzzle is this: find a number, called a **nonce**, that makes the block's digital fingerprint, its **hash**, fall below a target value. There is no way to calculate the answer in advance. You can only keep guessing, which means the only way to win is to do enormous amounts of work. That work is called **Proof of Work**, and the wasted-looking electricity is the entire security model. Rewriting history would mean redoing all that work, faster than every honest miner on Earth combined. That is what makes cheating not just hard but wildly expensive.



Reading the diagram, left to right. Pending payments wait in the **mempool** (the network's holding area for unconfirmed transactions). Miners race to solve the puzzle, each burning electricity guessing. The winner adds the new block (shown in gold, the settled state used across all five diagrams). Then time does the rest: each block stacked on top buries the transaction deeper, and after about six blocks (roughly an hour) it is considered settled.[1] Notice the finality is **probabilistic**, it gets safer with time rather than flipping to "done" instantly.

Probabilistic finality, or why you wait an hour

Finality is the moment a payment can no longer be undone. Bitcoin's version is unusual: a transaction is never stamped "certified final." Instead it becomes harder and harder to reverse as more blocks pile on top of it. One block deep, it is very likely permanent. Six blocks deep, about an hour later, reversing it would be so costly it is treated as settled. This is why exchanges make you wait for confirmations on large amounts. The payment is not getting more "approved," it is getting more buried.

Why miners stay honest

Each winning miner collects a **block reward**, newly issued bitcoin, plus the fees attached to the transactions they include. Playing by the rules pays a steady income. Attacking the network would cost more in electricity than it could ever steal, and would destroy the value of the very coins the attacker holds. The incentives are arranged so that honesty is simply the more profitable choice. That is the quiet genius of the design.

WHAT IT IS GOOD AT

- The longest unbroken track record of any network, securing its ledger since it launched.
- Truly open: anyone can mine or run a node, with no permission and no gatekeeper.
- A fixed, predictable issuance schedule no committee can change on a whim.

WHAT IT SACRIFICES

- Speed. Roughly ten minutes per block, and an hour for high-confidence settlement.
- Energy. The security comes from genuinely large electricity use.
- Flexibility. Its scripting is deliberately limited, so it is not a platform for complex apps.

UNLOCKS A censorship-resistant store of value and final settlement of large amounts. The thing it does best is simply being extremely hard to stop, change, or seize.

NOT BUILT FOR Fast everyday retail payments or rich on-chain applications. Bitcoin chose to be simple and unbreakable rather than fast and clever.

LEARN MORE

- The original Bitcoin whitepaper by Satoshi Nakamoto. Short, readable, and the source of it all (bitcoin.org/bitcoin.pdf).
- 3Blue1Brown, "But how does Bitcoin actually work?" The clearest visual explainer of the puzzle and the chain.
- Bitcoin.org, "How it works." Plain-language basics with no jargon.

NETWORK 02 / 05

Ethereum

PROOF OF STAKE

Replace the electricity with a cash bond, then turn the secured ledger into a programmable world computer.

WHERE IT LEANS · DIRECTIONAL, NOT A SCORE

* Decentralization is a theoretical ceiling. A large and growing share of staked ETH sits with a few staking pools and providers, which concentrates influence.

Ethereum

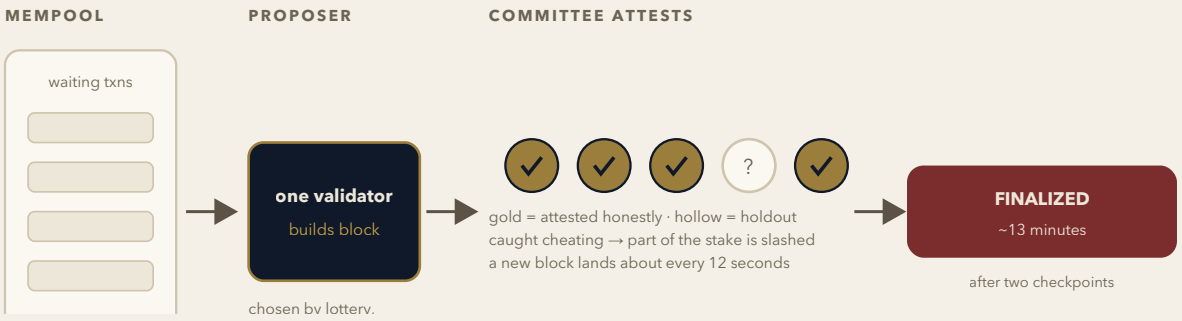
PROOF OF STAKE · ETH

A world computer. Trades a little speed and a lot of simplicity for the ability to run programs.

The mechanism, by analogy

Ethereum asks a sharp question: do we really need to burn electricity to make cheating expensive? Its answer is no, just make people put money on the line instead. Picture a voting pool where, to get a vote, you first post a sizable cash bond. If you vote honestly, you earn a little. If you are caught cheating, the pool keeps part of your bond.

To become a **validator** on Ethereum, you lock up 32 ETH as a security deposit.[2] Locking up coins this way is called **staking**. The network randomly picks one validator to propose the next block, and a committee of others to check it and vote that it is valid. Voting yes on a good block is called an **attestation**. Behave well and you collect modest rewards. Try to cheat by signing two conflicting versions of events, and the network destroys part of your stake. That punishment is called **slashing**, and it replaces electricity as the cost of dishonesty. Going offline is treated far more gently: you miss rewards and slowly leak a little stake while away. Slashing is reserved for provable foul play. Your own money is the thing at risk.



Reading the diagram. One validator is chosen to propose a block, weighted by how much is staked. A committee then votes (the gold checks are agreement, the hollow one is a holdout), and any validator caught cheating gets **slashed**, its stake partly burned. A new block appears about every **12 seconds**, but the network only calls a block **finalized**, meaning economically irreversible, once enough votes accumulate, roughly **13 minutes** later.

Twelve seconds versus thirteen minutes

This is the distinction that trips people up. A new block lands about every twelve seconds, so your transaction usually appears on the chain quickly. But appearing is not the same as being final. Ethereum reaches full **finality** in two steps. It marks a checkpoint about every six and a half minutes, and a block is only locked in for good after two checkpoints have passed. Two of those, back to back, is where the

familiar thirteen-minute figure comes from.[3] Fast to show up, slower to become truly permanent. Both numbers are normal, they simply describe different moments.

What staking unlocks: programmability

Ethereum's real breakthrough is not the consensus method, it is what the consensus secures. Ethereum runs **smart contracts**, self-executing programs that live on the chain and run exactly as written, with no company in the middle able to alter or stop them. A smart contract can hold funds, enforce an agreement, or run an entire application. This is why Ethereum is described less as digital gold and more as a world computer. Most of what people mean by "crypto apps," lending, stablecoins, digital collectibles, exchanges that run without a company, was built on this foundation.

WHAT IT IS GOOD AT

- Energy-light: no electricity race, just bonded capital at risk.
- Programmable: a full platform for applications, not just a coin.
- A large, globally distributed set of validators securing it.

WHAT IT SACRIFICES

- Simplicity. More moving parts means more things that can go wrong, including buggy contracts.
- Base-layer speed and cost. Busy periods push fees up, which is why "layer 2" helper networks exist.
- Final settlement is slower than the newest chains.

UNLOCKS Smart contracts and an entire ecosystem of applications built on top of them. If a crypto product is doing something more complex than sending a coin, it very likely started here.

NOT BUILT FOR Maximum raw throughput at rock-bottom cost on the base layer. That job is increasingly handed to **layer 2** networks, extra layers that bundle activity and settle back to Ethereum.

LEARN MORE

- Ethereum.org, "Proof of stake (PoS)." The official, plain-language walkthrough of staking and slashing.
- Finematics (YouTube). Animated explainers of smart contracts and the apps built on them.
- Ethereum.org, "Intro to Ethereum." Good grounding before the deeper material.

NETWORK 03 / 05

XRP

BYZANTINE FAULT TOLERANCE · RPCA

Let a circle of trusted validators agree in seconds, settling value with final, low-cost simplicity.

WHERE IT LEANS · DIRECTIONAL, NOT A SCORE

SECURITY	■■■□
DECENTRALIZATION	■■□□
SCALABILITY	■■■□

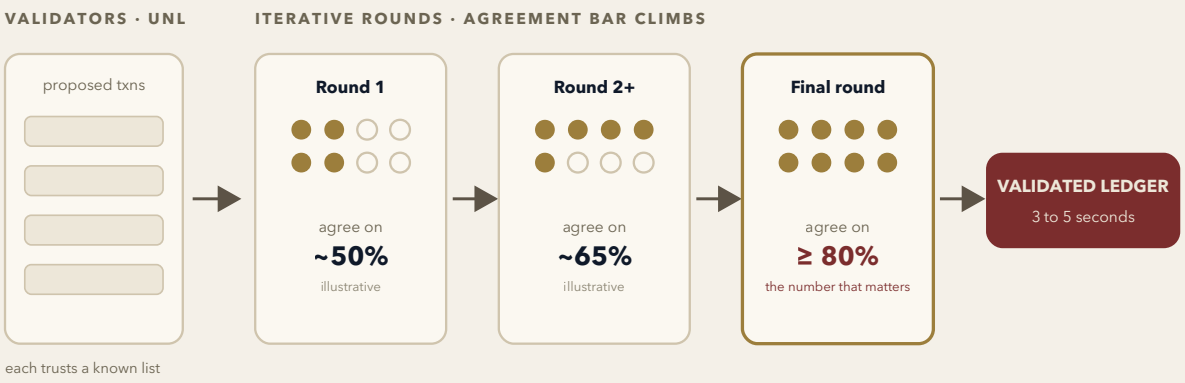
XRP

A circle of trusted validators that settles value in seconds. No mining, no race.

The mechanism, by analogy

XRP does not use a race at all. Its method belongs to a family called **Byzantine Fault Tolerance**, the ability of a system to reach a correct, shared answer even if some participants are broken or actively lying. The name comes from a classic puzzle about generals trying to coordinate an attack while some of them are traitors sending false messages. The specific recipe XRP uses is the **Ripple Protocol Consensus Algorithm**, or RPCA.

Picture a room of people, each of whom trusts a known list of respected colleagues. Every few seconds, they each propose which transactions should go in the next batch. They look at what everyone else proposed, drop anything that is not widely shared, and propose again. They keep adjusting through several quick rounds, and the bar for agreement rises each round, until at least 80% of their trusted colleagues have landed on the exact same set. At that point the batch is locked into the ledger. No puzzles, no electricity, just rapid rounds of "here is my list, let me see yours, let me adjust."



Reading the diagram. Validators start by agreeing on a rough set of transactions, then re-propose through several fast rounds. The early percentages are illustrative, drawn to show how the agreement bar climbs; the **80% supermajority** is the real number that matters. Once they clear it, the ledger is **validated** and settlement is final in about three to five seconds.[4] Gold dots are validators that have converged, hollow dots have not yet.

Quorum intersection, in plain English

Here is the clever part that keeps it from breaking. Each validator follows a list of validators it chooses to trust, called a **Unique Node List**, or UNL. The safety of the whole system rests on a simple fact: these lists heavily overlap. Because almost everyone's trusted set shares most of the same members, the network does not split into two groups that each believe they reached agreement on different answers, as long as those trusted lists overlap enough. That overlap is the glue. A ledger splitting into two conflicting versions is called a **fork**, and keeping the trusted lists heavily overlapped is what prevents one. The safety is strong but conditional: it depends on that overlap holding, not on a law of physics. To make this easy to set up, the **XRPL Foundation** publishes a recommended validator list, so operators do not each have to assemble trust from scratch.

No subsidy, and an honest limit that is shifting

There is no mining reward and no staking payout here. All XRP was created at the start, so validators are not paid in new coins. They run for reliability and reputation, not a prize, and a tiny fee on each transaction is destroyed rather than paid out. On programmability, the picture is changing. The base ledger is gaining native programmability built on **WebAssembly** (a fast, portable way to run small programs), rolling out in deliberate phases: simpler programmable features are already live, while broader native smart-contract support is in active development on test networks. A separate **EVM sidechain**, a companion network that speaks Ethereum's language, also exists for Solidity-style apps. Even so, the honest framing holds: the base ledger still favours a focused set of fast, purpose-built primitives over being a general world computer like Ethereum, and full native programmability is maturing rather than finished.

WORTH CHECKING XRP Ledger programmability is rolling out in phases and is actively evolving. The direction (native WebAssembly programmability plus a separate Ethereum-compatible sidechain) is set, but exactly which capabilities are live versus still on test networks shifts over time. Confirm the current state before relying on any specific feature.

WHAT IT IS GOOD AT

- Speed. Final settlement in roughly three to five seconds.
- Fast and final once validated. The safety rests on trusted lists overlapping as assumed.
- Cheap and energy-trivial: no mining, no staking machinery.

WHAT IT SACRIFICES

- Openness. Trust rests on curated validator lists, which is more coordinated than open mining.
- Native programmability is still maturing, so the base ledger favours a focused set of primitives.
- A perception of central involvement that some hold against it.

UNLOCKS Fast, cheap, final settlement of value, with cross-border payments as the headline use case. It is purpose-built to move money quickly.

NOT BUILT FOR Heavy, general-purpose app development on the base ledger, at least for now. Native programmability is arriving in phases rather than being a finished, all-purpose platform like Ethereum.

LEARN MORE

- XRPL.org, "Consensus" and the developer docs. The official, technical-but-readable description of the rounds, the UNL, and programmability.
- The XRPL Foundation. Publishes the recommended validator list and neutral documentation.
- Talks by David Schwartz on XRP Ledger consensus. From one of the original designers.

NETWORK 04 / 05

Solana

PROOF OF HISTORY + PROOF OF STAKE

Timestamp every transaction the moment it arrives, so ordering is solved before anyone votes and the speed follows.

WHERE IT LEANS · DIRECTIONAL, NOT A SCORE

* Scalability is a theoretical peak. Multiple network outages have interrupted finality and reduced real-world throughput reliability.

Solana

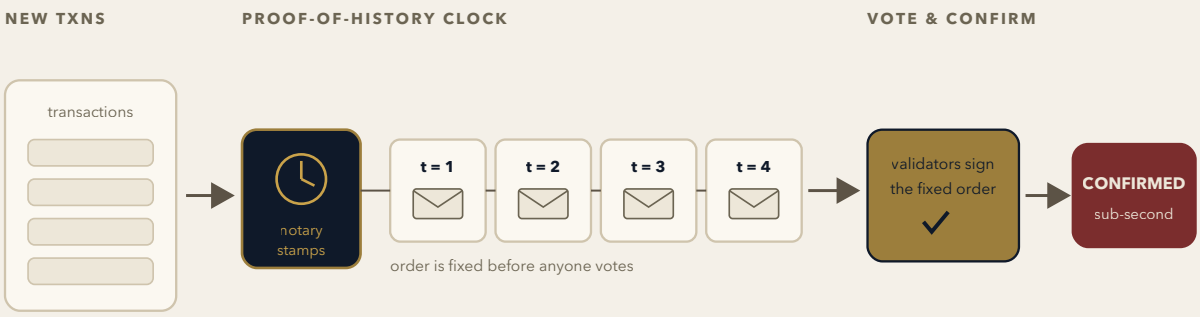
POH + POS · SOL

Built for raw speed. Timestamps everything up front so validators never argue about order.

The mechanism, by analogy

In most networks, the slowest and most argument-prone part of consensus is agreeing on the order of events. Whose transaction came first? Solana's insight is to settle the order before anyone votes. Picture a notary who stamps an exact time on every envelope the instant it arrives, before any of it goes into the pile. Later, nobody has to argue about sequence, because the stamps already prove it.

That notary is called **Proof of History**. It is not a consensus mechanism on its own, it is a clock. It works by running a continuous chain of computed timestamps, each one provably built on the last, so the network can show that event B happened after event A without validators ever comparing their watches. On top of that clock, Solana runs a **Proof of Stake** voting system of its own, called Tower BFT: validators stake coins and vote to confirm the already-ordered stream, with more stake carrying more weight. Going offline or missing votes costs a validator rewards. The clock does the ordering, the staked voting secures it.



Reading the diagram. As transactions arrive, the Proof-of-History "notary" stamps each one with a verifiable time (t=1, t=2, t=3...), producing a single pre-ordered stream. Because the order is already fixed, validators do not debate sequence, they simply vote to confirm a stream that is settled (the gold confirmation). That removed argument is where the **sub-second** speed comes from.

Confirmed is not the same as final

Solana separates two moments, much as Ethereum does. A transaction is confirmed in well under a second, as soon as a supermajority of validators has voted for the block it sits in. That fast confirmation is what makes the network feel instant. But confirmation is not full finality. A block is only treated as **finalized**, rooted so deeply that the network will not roll it back, once about another thirty blocks have

been built and voted on top of it, which takes roughly thirteen seconds.[5] Sub-second is the confirmation you see; the firmer guarantee lands a little after. Both numbers are normal, they simply describe different moments.

The speed, and the honest trade-off

The payoff is dramatic. Solana can process very high volumes of transactions, confirming in well under a second to a few seconds, at very low fees. For applications that need to feel as instant as a normal app, that matters.

Now the honest part. That speed has costs that are easy to skip past. Keeping up with the firehose of timestamped transactions demands powerful, expensive hardware, which means there are fewer validators than on Bitcoin or Ethereum. Fewer validators is a real decentralization trade-off. And the network is younger and has had **outages**, periods where it stopped producing blocks and had to be restarted by its operators.[6] It is fast and steadily improving, but it does not yet have the long "nothing has ever stopped it" track record that Bitcoin can point to.

WHAT IT IS GOOD AT

- Extreme throughput and sub-second confirmation at very low cost.
- Fully smart-contract capable, so it hosts real applications.
- A snappy, consumer-app feel that slower chains struggle to match.

WHAT IT SACRIFICES

- A high hardware bar, which means fewer validators and more centralization pressure.
- A shorter track record, including several network outages.
- Less of the "anyone on a laptop can join" character.

UNLOCKS High-volume, low-cost applications at scale: fast trading, payments, and consumer-facing apps where speed and tiny fees are the whole experience.

NOT BUILT FOR The maximal "it has never once stopped" reliability story. Solana is betting that performance, refined over time, is worth a younger and more demanding design.

LEARN MORE

- Solana.com docs, "Proof of History." The official description of the timestamp clock.
- Anatoly Yakovenko's original Proof of History write-up. From Solana's founder, where the idea was introduced.
- Helius blog, Solana explainers. Clear, current breakdowns of how the network runs.

NETWORK 05 / 05

Hedera

HASHGRAPH · DAG

Drop the single chain of blocks. Let a gossiping web converge on order, fast and mathematically final.

WHERE IT LEANS · DIRECTIONAL, NOT A SCORE

* Both bars are theoretical ceilings. The asynchronous BFT guarantee is the strongest category on paper, but in practice it rests on a small, permissioned set of council-run nodes, not an open crowd, and real-world throughput has run well below the headline figure.

Hedera

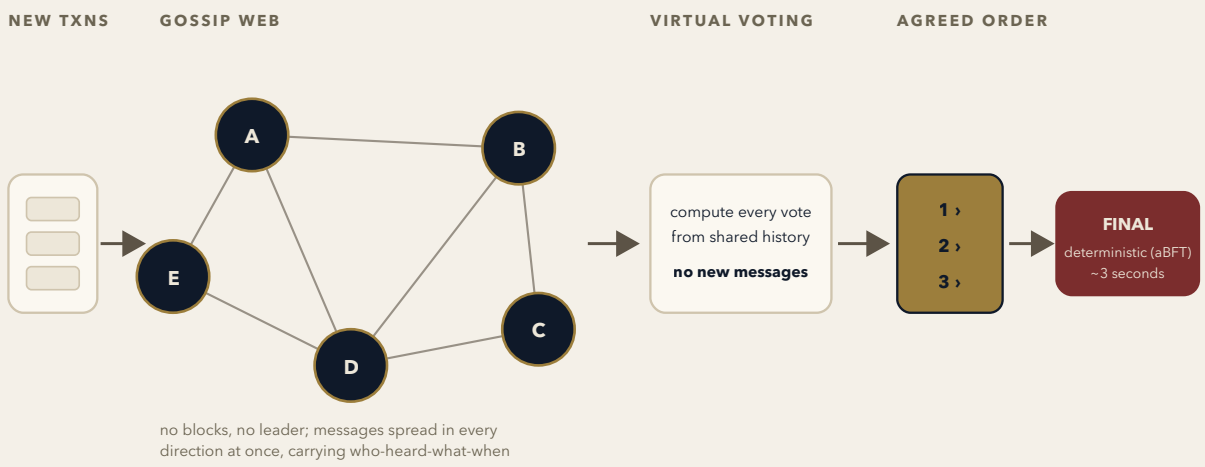
HASHGRAPH / DAG · HBAR

A fundamentally different shape. No chain of blocks at all, but a gossiping web.

The mechanism, by analogy

Every network so far builds a single line of blocks, one at a time. Hedera throws that picture out. Its structure is a **Directed Acyclic Graph**, or DAG, a web of connected events that all flow forward in time and never loop back on themselves. Instead of one straight chain, imagine a spreading web.

Here is how it fills in. There is no winner and no leader. Instead, every node constantly **gossips**. When two nodes connect, each tells the other everything it has heard and exactly when it heard it. Crucially, they also pass along the fact that they passed it along, a record of who told whom, when. This is called **gossip about gossip**. Very quickly, every node ends up holding the same complete web of who-heard-what-and-when. And because they all share that identical history, each node can calculate how every other node would vote on the ordering of events, without sending a single additional message. Working out the result from shared history alone is called **virtual voting**, and skipping the extra round of messages is a big part of why it is fast.



Reading the diagram. This is the "different shape" entry, so look at the middle. There is no line of blocks. Nodes A through E **gossip** in every direction at once, each message carrying a record of who heard what and when. Because every node ends up with the same web of history, it can run **virtual voting** (compute everyone's vote) with no new messages, producing a single agreed order. Finality is **deterministic**: once ordered, it is mathematically final, never just "probably."

Parallel, not sequential

This is the key divergence worth holding onto. A blockchain is sequential: one block at a time, built by one participant at a time, with everyone else waiting. A hashgraph is parallel: messages from everyone flow at once and get woven into a single agreed order afterward. The shape is a web, not a chain. On security, Hedera uses what is, on paper, the strongest category of Byzantine Fault Tolerance, called **asynchronous BFT**, and its finality is deterministic, settled in a few seconds with a mathematical guarantee rather than a probability that grows over time.

The governance trade-off, stated plainly

Speed and efficiency come with a deliberate choice about who runs the network. Hedera's nodes are operated by the **Hedera Governing Council**, a fixed group of up to several dozen large, named organizations that take turns running the infrastructure. This makes the network stable, accountable, and predictable, you know exactly who the operators are. But it is **permissioned**: you cannot simply spin up a council node the way anyone, anywhere, can start mining Bitcoin. That is the honest trade-off. Hedera deliberately limits how open its governance is, in exchange for speed, efficiency, and predictable performance.

WHAT IT IS GOOD AT

- Very fast and final, with deterministic settlement in seconds.
- Tiny energy use and predictable, very low fees.
- Strong security guarantees (asynchronous BFT) and named, accountable operators.

WHAT IT SACRIFICES

- Open participation. A permissioned council runs the nodes, the most curated of the five.
- A younger, smaller ecosystem than the older networks.
- The "anyone can validate" ethos that defines permissionless chains.

UNLOCKS Enterprise-grade, high-volume uses, payments, asset tokenization, and tamper-proof logging, where predictable performance and known, accountable operators are a feature rather than a flaw.

NOT BUILT FOR The permissionless, anyone-can-join-and-validate ideal that Bitcoin holds as its core value. Hedera trades that openness for performance and accountability.

LEARN MORE

- Hedera.com Learning Center, "Hashgraph" and "Gossip about gossip." The official, beginner-friendly explanations.
- Leemon Baird's hashgraph papers and talks. From the algorithm's inventor, including clear animations.
- Visual "hashgraph explained" walkthroughs. Helpful for seeing the web form, since the shape is the hard part.

SECTION 03

The five at a glance

This scorecard is shorthand, and it only works because the pages before it did the real explaining. Read each cell as a pointer back to a nuance you now understand, not as a ranking. None of these is "winning." They are built for different jobs.

	Bitcoin BTC	Ethereum ETH	XRP XRP	Solana SOL	Hedera HBAR
CONSENSUS TYPE	**Proof of Work**	**Proof of Stake**	**Byzantine Fault Tolerance (RPCA)**	**Proof of History on Proof of Stake**	**Hashgraph (gossip + virtual voting)**
PROBLEM IT SOLVES BEST	Unstoppable, censorship-resistant store of value	Programmable money and on-chain apps	Fast, final settlement of value across borders	High-volume, low-cost apps that feel instant	Predictable high-volume use with named operators
FINALITY SPEED	~1 hour (6 blocks, probabilistic)	~13 minutes (economic finality)	~3 to 5 seconds (final)	~1 sec to confirm, ~13 sec to finalize*	~3 seconds, often faster (deterministic)
ENERGY USE	**Very high**	Low	Very low	Low to moderate	Very low
DECENTRALIZATION (OPENNESS TO JOIN)	▮▮▮▮ ** Most open; anyone can mine, though pools concentrate power	▮▮▮▯ *** Broad validator set; staking can concentrate	▮▮▯▯ Curated trusted-validator lists	▮▮▯▯ Fewer validators due to hardware demands	▮▯▯▯ Permissioned council; most curated

The meter shows how open each network is to anyone joining as a validator: more bars, more open. It is a rough cue, not a grade. Every position here is a deliberate trade made to be better at something else.

Scorecard accurate as of June 2026. Ratings reflect theoretical capabilities balanced against observed network conditions. See asterisks for specific caveats.

* Solana finality and throughput. Solana targets 10,000+ TPS theoretically. However, the network's operational history includes multiple outages that have interrupted finality and reduced throughput reliability.

** Bitcoin decentralization. Anyone can mine in principle, but in practice a small number of mining pools command most of the network's hashrate. That concentrates who actually builds blocks, even though running a node stays open to all.

*** Ethereum decentralization. The protocol allows broad, permissionless validation, but a large and growing share of staked ETH sits with a few staking pools and providers. That concentrates influence despite the open design.

THE ONE IDEA TO CARRY AWAY

There is no best consensus mechanism, only different bets on security, speed, decentralization, and programmability. When you understand which bet a network made, you understand what it is genuinely useful for, and you stop comparing a vault to a sports car as if one is simply wrong.

Educational only. This guide is a plain-English explainer of how these networks reach agreement. It is not investment, financial, tax, legal, or technical advice, and it does not recommend buying, selling, or holding anything. The five networks were chosen for the diversity of their consensus designs, not for size, ranking, or any view on their merit as investments. Use it to understand the technology and to ask sharper questions of qualified professionals. Position Clarity is not registered with any Canadian securities regulator.

How these ratings are set. The bars and meters throughout this guide are our qualitative reading of recognized indicators, not a single published score, and no agreed cross-network scale exists. Decentralization draws on the Nakamoto Coefficient and stake or hashrate concentration (see the Edinburgh Decentralisation Index and clientdiversity.org). Security draws on cost-to-attack estimates and length of track record (see crypto51.app). Scalability draws on observed versus theoretical throughput and finality (see chainspect.app). These indicators move over time, so read the bars as direction, not measurement.

Sources

Each network's timing and mechanism claims were checked against primary or official sources. These figures are perishable, since networks change their parameters, so they were verified as of June 2026. Confirm current status before relying on a number.

1. Bitcoin Wiki, *Confirmation.* Six confirmations is a long-standing convention for treating a payment as settled; the whitepaper sets no fixed number, only that reversal odds fall with each block. en.bitcoin.it
2. Ethereum Foundation, *Staking.* Running a validator requires depositing 32 ETH, which can be reduced by penalties or slashing. ethereum.org/staking
3. Ethereum Foundation, *Proof of stake.* A 12-second slot, a 32-slot epoch, and finality across two consecutive epochs (roughly 13 to 15 minutes). ethereum.org
4. XRP Ledger Documentation, *Consensus.* Agreement needs at least 80 percent of trusted validators, and ledgers usually close every 3 to 5 seconds. xrpl.org
5. Solana Developers, *Transaction Confirmation.* A block is finalized once about 31 more confirmed blocks are built on top, roughly 13 seconds. solana.com
6. Solana network outage history (Helius, and Solana status records). The network has had multiple outages where block production stopped and was restarted. helius.dev

As of June 2026. Confirm current status; consensus parameters and network conditions change.

Position Clarity

Plain-English crypto education, so you understand what you own and know what to ask next.

positionclarity.ca

positionclarity.ca/contact